Analytic orders for Tate–Shafarevich groups and regulators of lower-rank quadratic twisted elliptic curves

Shenghao Hua
Shandong U & EPFL

Aarhus Automorphic Forms Conference

Outline

Definition

Elliptic curve

An elliptic curve E over field K is the set of soultions of an equation of the form

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy + J = 0,$$

and all coefficients are in K.

Weierstrass form

After linear changing of variables, E can be written in the form

$$y^2 = x^3 + ax + b,$$

with $a, b \in K$. This type of equation is called a Weierstrass normal form.

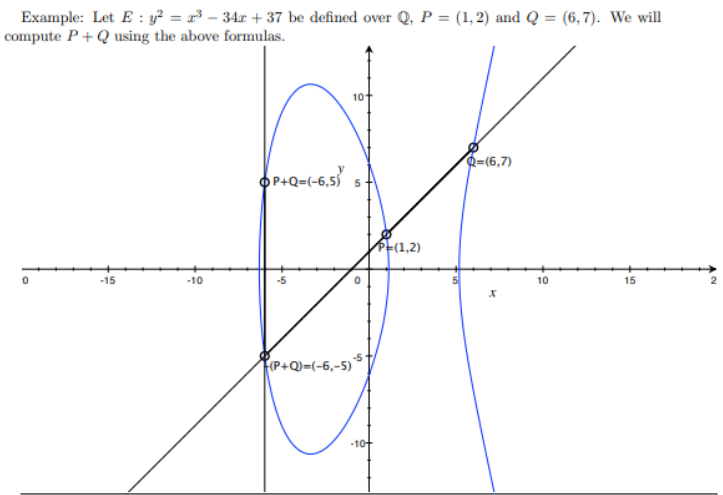
Here we let $\Delta(E) = -16(4a^3 + 27b^2) \neq 0$, then the elliptic curve has curve genus 1.

Group law

Take 2 points P and Q. Now "draw" a straight line through them and compute the third point of intersection R, set infinity be the identity point,

$$P + Q + R = 0,$$

and the inverse of $R = (x, y)$ is $-R = (x, -y)$.



(Image produced by Ashley Neal)

Mordell–Weil group

Mordell–Weil theorem

Let K be an finitely extension field of $\mathbb{Q}$. The group $E(K)$ of K-rational points is a finitely–generated abelian group, called the Mordell–Weil group.

$$E(K) \cong E(K)_{\text{tors}} \times \mathbb{Z}^r,$$

where $E(K)_{\text{tors}}$ is the torsion subgroup, in which every element has finite order, and r is the (algebraic) rank of $E(K)$.

Mazur: $E_{\text{tors}}(\mathbb{Q})$ is one of 15 possible groups
Kenku–Momose, Kamienny: for quadratic field K, $E_{\text{tors}}(K)$ is one of 18 possible groups
The maximal free subgroup of $E(K)$ is a lattice, with the volume $\mathrm{Reg}(E/K)$, with some kind of "canonical height" (Néron–Tate height).

Local-Global obstruction

Global→ Local

For index set I, rational equations

$$f_i(x_1, \ldots, x_n) = 0, \quad (i \in I)$$

have K solutions only if they have solutions in every (∞ or finite) places of K.

Could us go back (Local→ Global)?

Local-Global obstruction

Global→ Local

For index set I, rational equations

$$f_i(x_1, \ldots, x_n) = 0, \quad (i \in I)$$

have K solutions only if they have solutions in every (∞ or finite) places of K.

Could us go back (Local→ Global)?

Tate–Shafarevich group

$$Ш(E(\mathbb{Q})) := \cap_v \ker(\mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E) \to \mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}_v}/\mathbb{Q}_v), E),$$

is the quotient from local to global.

Tate–Shafarevich group

Questions

How large it is? How it looks like?

Tate–Shafarevich group

Questions

How large it is? How it looks like?

Tate–Shafarevich conjecture

For any K and $E(K)$, it's finite group.

Tate–Shafarevich group

Questions

How large it is? How it looks like?

Tate–Shafarevich conjecture

For any K and $E(K)$, it's finite group.

Cassels's pairing

There is an alternating bilinear pairing

$$\langle \cdot, \cdot \rangle : Ш(E) \times Ш(E) \to \mathbb{Q}/\mathbb{Z},$$

which is non-degenerate assuming $Ш(E)$ is finite. Then there exists an isotropic subgroup $H(E) \subseteq Ш(E)$, meaning that $\langle x, y \rangle = 0$ for all $x, y \in H(E)$, with $\#H(E)^2 = \#Ш(E)$, and such subgroups generate $Ш(E)$.

Tate–Shafarevich group

Questions

How large it is? How it looks like?

Tate–Shafarevich conjecture

For any K and $E(K)$, it's finite group.

Cassels's pairing

There is an alternating bilinear pairing

$$\langle \cdot, \cdot \rangle : Ш(E) \times Ш(E) \to \mathbb{Q}/\mathbb{Z},$$

which is non-degenerate assuming $Ш(E)$ is finite. Then there exists an isotropic subgroup $H(E) \subseteq Ш(E)$, meaning that $\langle x, y \rangle = 0$ for all $x, y \in H(E)$, with $\#H(E)^2 = \#Ш(E)$, and such subgroups generate $Ш(E)$.

Gross–Zagier 1986, Kolyvagin 1990

For modular elliptic curves with $\mathbb{Q}$-rational coefficients and analytic rank at most 1, its Tate–Shafarevich group a finite group.

Hasse–Weil L-function of E

Take $a_{\mathfrak{p}} = \mathrm{N}(\mathfrak{p}) + 1 - \#E(\mathcal{O}_K/\mathfrak{p})$, the Hasse–Weil L-function of E over K with central point at 1 is

$$L(s, E/K) = \prod_{\mathfrak{p}} \frac{1}{1 - a_{\mathfrak{p}} \mathrm{N}(\mathfrak{p})^{-s} + \mathrm{N}(\mathfrak{p})^{1-2s}}, \quad \mathrm{Re}(s) \gg 1,$$

Thanks to the modularity theorem (Wiles 1995, Diamond 1996, Conrad–Diamond–Taylor 1999, Breuil–Conrad–Diamond–Taylor 2001), we have the functional equation and analytic continuation for Hasse–Weil L-function for elliptic curves with $\mathbb{Q}$-rational coefficients.

Analytic rank

The vanishing order of $L(s, E/K)$ at central point is the so-called analytic rank.

Gross–Zagier 1986, Kolyvagin 1990

Let $K = \mathbb{Q}$, when analytic rank ≤ 1, we have algebraic rank equals to analytic rank.

Birch and Swinnerton-Dyer conjecture

For E over number field K,

$$\lim_{s \to \text{central}} \frac{L(s, E/K)}{(s - \text{central})^r} = \frac{\#Ш(E/K)\,\mathrm{Reg}(E/K)\Omega_{E/K} \prod_{v \text{ finite}} \mathrm{Tam}_v(E(K))}{(\#E(K)_{\text{tors}})^2},$$

where:

- $r = \mathrm{ord}_{\text{central point } s} L(E/K, s)$ is the analytic rank of E,
- $Ш(E/K)$ is the Shafarevich–Tate group,
- $\Omega_{E/K} = \prod_{v|\infty} \int_{E(K_v)^0} |\omega|$ is the product of the real or complex periods at the archimedean places,
- $\mathrm{Tam}_v(E(K))$ are the Tamagawa numbers at the finite places v of K,
- $E(K)_{\text{tors}}$ is the torsion subgroup of $E(K)$.

Quadratic twists of E

Let $K = \mathbb{Q}$. Let E be an elliptic curve of the form

$$y^2 = x^3 + ax + b.$$

Given square-free d, the quadratic twist of E is the curve $E^{(d)}$, defined by the equation

$$y^2 = x^3 + ad^2x + bd^3.$$

For $\mathrm{Re}(s) \gg 1$

$$L(s, E) = L(s, E/\mathbb{Q}) = \sum_{n=1}^{\infty} a(n)n^{-s} \Rightarrow L(s, E^{(d)}) = \sum_{n=1}^{\infty} a(n)\chi_d(n)n^{-s}$$

For $d < 0$, we have base change L-function

$$L(s, E/\mathbb{Q}(\sqrt{d})) = L(s, E)L(s, E^{(d)}).$$

We normalize the central point to $s = \frac{1}{2}$.

Analytic rank 0: Admissible congruence classes

Let

$$\Omega := \{d : \mu(d)^2 = 1,\ (d, 2N) = 1, \epsilon_{E^{(d)}} = \epsilon_E \chi_d(-N) = 1\}.$$

Let $N_0 = [8, N]$. Let $\sigma \in \{\pm 1\}$ and $a \pmod{N_0}$ denote a residue class with $a \equiv 1 \pmod 4$. We assume that σ and a are such that for any fundamental discriminant d of sign σ with $d \equiv a \pmod{N_0}$, the root number $\epsilon_{E^{(d)}} = 1$. Define

$$\Omega(a, \sigma) := \{d \in \Omega :\ d \equiv a \pmod{N_0},\ \sigma d > 0\}.$$

Analytic rank 0: Analytic order of $Ш(E^{(d)})$

For $d \in \Omega$, then

$$S(E^{(d)}) = L\left(\frac{1}{2}, E_{E^{(d)}}\right) \frac{|E^{(d)}(\mathbb{Q})_{tors}|^2}{\Omega(E^{(d)})\,\mathrm{Tam}(E^{(d)})}.$$

If $L(\frac{1}{2}, E^{(d)}) \neq 0$, then the Birch and Swinnerton-Dyer conjecture predicts that $S(E^{(d)}) = Ш(E^{(d)})$.

Order of real period (Pal 2012)

For square-free $(d, 2N) = 1$, the real period $\Omega(E^{(d)})$ satisfies

$$\Omega(E^{(d)}) = \frac{\tilde{u}}{\sqrt{|d|}}\Omega(E)$$

with some $\tilde{u} \in \frac{1}{2}\mathbb{Z}$ only decided by E.

Radziwiłł–Soundararajan 2015 & 2024

Assuming the BSD conjecture (and the GRH), we have one-sided (two-sided) central limit theorem for $\log\left(Ш(E^{(d)})\,\mathrm{Tam}(E^{(d)})\right)$ with $d \in \Omega(a, \sigma)$.

A barrier

We have $\mathrm{Tam}_p(d) = 1$ for $p \nmid dN_0$, $\mathrm{Tam}_p(d)$ is fixed for $p \mid N_0$ even if d changes, and $\mathrm{Tam}_p(d) \in \{1, 2, 4\}$ for $p \mid d$.

trivial bound

$\tau(d)$ has the extremal large order as

$$\exp(\log 2 \frac{\log d}{\log \log d}).$$

Conjecture (Farmer–Gonek–Hughes 2007)

$$\max_{d \le D} |L(\frac{1}{2}, E^{(d)})| = \exp((1 + o(1))\sqrt{\log D \log \log D}).$$

Extreme analytic order of $Ш(E^{(d)})$

H.–Huang (arXiv: 2212.13360)

For any fixed $W \geq 20$ and any odd a coprime to the conductor of E, we have

$$\max_{\substack{d \in \Omega(a,\sigma) \\ \frac{D}{2} \leq |d| \leq \frac{5D}{2} \\ \omega(d) \leq W}} S(Ш(E^{(d)}) \geq \sqrt{D} \exp\left(\left(2\sqrt{\frac{W - 19.73}{22W + 12}} + o(1) \right) \frac{\sqrt{\log D}}{\sqrt{\log\log D}} \right),$$

as $D \to \infty$.

Reference:

Hua, Shenghao; Huang, Bingrong. Extreme central L-values of almost prime quadratic twists of elliptic curves. *Sci. China Math.* 66 (2023), no. 12, 2755–2766. (Dedicated to the 50th anniversary of Jing-run Chen's Theorem $(1 + 2)$ on the Goldbach Conjecture)

Decorrelation of analytic order of isotropy subgroups of $Ш(E^{(d)})$

H. (arXiv this week)

Let $1 \leq i \leq m$, and suppose each conductor N_i elliptic curve E_i is associate to a weight two Hecke eigenform f_i with root number ϵ_{f_i}. Fix $\sigma = \pm 1$. Let $N_0 = [8, N_1, \ldots, N_m]$. Let $a \bmod N_0$ denote a residue class with $a \equiv 1 \pmod 4$ and $(a, N_0) = 1$ and for every fundamental discriminant $\sigma d > 0$ with $d \equiv a \pmod{N_0}$, the root numbers satisfy $\epsilon_{f_i}(d) = \epsilon_{f_i}\chi_d(-N_i) = 1$, for all $i = 1, \ldots, m$.
Assume the GRH holds for $L(s, \mathrm{sym}^2 f_i)$ and $L(s, f_i \times \chi_d)$ for all f_i and for all $D \leq \sigma d \leq 2D$ with $d \equiv a \pmod{N_0}$, and the BSD conjecture holds for $E_i^{(d)}$. For any $\varepsilon > 0$, we have

$$\frac{1}{D} \sum_{\substack{D \leq \sigma d \leq 2D \\ \mu(|d|)^2 = 1 \\ d \equiv a \pmod{N_0}}} \prod_{i=1}^{m} \frac{\delta_{r(E_i^{(d)}=0)} \# H(E_i^{(d)})}{|d|^{1/4}} \ll_{E_1, \ldots, E_m, \varepsilon} (\log D)^{-\frac{m}{8} + \varepsilon}.$$

Decorrelation of mixed moments for quadratic twisted L-Functions

H. (arXiv this week)

- Decorrelation of quadratic twisted central L-values of even-weight Hecke eigenform or a Hecke–Maass form satisfying the Generalized Ramanujan Conjecture (GRC).
- Decorrelation of automorphic periods averaged over imaginary quadratic fields.
- Decorrelation of Fourier coefficients of half-integral weight modular forms.

Decorrelation of mixed moments for orthogonal families of L-Functions

Keating–Snaith conjecture / Katz–Sarnak philosophy

For orthogonal families of L-functions, the moments of central values in the range between order 0 and 1 (excluding the endpoints) contribute a negative power of $\log$ in their leading-order asymptotics.

Multiple automorphic forms share the same symmetry type

Chandee's work on shifted moments of the Riemann zeta function, and later the work of Milinovich and Turnage-Butterbaugh on integral moments of product of L-functions.

Applications

- Lester–Radziwiłł proved quantum unique ergodicity for half-integral weight automorphic forms.
- Huang–Lester investigated the quantum variance of dihedral Maass forms.
- Blomer–Brumley–Khayutin (newly) proved the joint equidistribution conjecture of Michel and Venkatesh.
- Blomer–Brumley proved arithmetic quotients orbits joint equidistribution.
- Jääsaari–Lester–Saha established sign changes for coefficients of Siegel cusp forms of degree 2.
- Jääsaari–Lester–Saha showed that the mass of Saito–Kurokawa lifted holomorphic cuspidal Hecke eigenforms for $\mathrm{Sp}_4(\mathbb{Z})$ equidistributes on the Siegel modular variety as the weight tends to infinity.
- **H.**–Huang–Li proof a case of our joint Gaussian moment conjecture.
- Huang established holomorphic version.
- Chatzakos–Cherubini–Lester–Risager obtained a logarithmic improvement on Selberg's longstanding bound for the error term in the hyperbolic circle problem over Heegner points with varying discriminants.
- **H.** demonstrated that for $0 < p < 2$, the ℓ^p-norm of some quadratic forms in holomorphic Hecke cusp forms tends to zero asymptotically.

Analytic rank 1: $\mathrm{Reg}(E/\mathbb{Q}(\sqrt{d}))$ and $\mathrm{Reg}(E^{(d)}/\mathbb{Q})$

Leibniz rule for imaginary quadratic field

$$L'(\frac{1}{2}, E/\mathbb{Q}(\sqrt{d})) = L(\frac{1}{2}, E)L'(\frac{1}{2}, E^{(d)}) + L'(\frac{1}{2}, E)L(\frac{1}{2}, E^{(d)})$$

Gross–Zagier formulas

Let E non-CM.
Heegner condition: $d < 0$, $d \equiv 1 \pmod 4$, and $(\frac{d}{q}) = 1$ for all $q \mid N$.
Then for $r(E) + r(E^{(d)}) = 1$, we have

$$L'(\frac{1}{2}, E/\mathbb{Q}(\sqrt{d})) = \frac{32\pi^2 \|f_E\|^2}{|\mathcal{O}^\times_{\mathbb{Q}(\sqrt{d})}|^2 \sqrt{|d|} \cdot \deg \phi_E} \cdot \widehat{h}_{\mathbb{Q}(\sqrt{d})}(P_{\mathbb{Q}(\sqrt{d})}),$$

and for $r(E) = 0$, $r(E^{(d)}) = 1$, we have

$$L'(\frac{1}{2}, E^{(d)}) = \frac{32\pi^2 \|f_E\|^2}{|\mathcal{O}^\times_{\mathbb{Q}(\sqrt{d})}|^2 \sqrt{|d|} \cdot \deg \phi_E} \cdot \widehat{h}_{\mathbb{Q}}(P_d).$$

Analytic rank 1: $\mathrm{Reg}(E/\mathbb{Q}(\sqrt{d}))$ and $\mathrm{Reg}(E^{(d)}/\mathbb{Q})$

H. (arXiv: 2507.20297)

For E non-CM, and d satisfies the Heegner condition.

- Handling some log contribution to get one-sided central limit theory for $\log \mathrm{Reg}(E/\mathbb{Q}(\sqrt{d}))$ and $\log \mathrm{Reg}(E^{(d)}/\mathbb{Q})$.
- Using Hölder's inequality to show lots of d such that $\mathrm{Reg}(E/\mathbb{Q}(\sqrt{d}))$ and $\mathrm{Reg}(E^{(d)}/\mathbb{Q})$ have size $\gg \sqrt{|d|}$.

Analytic rank 1: $\mathrm{Reg}(E/\mathbb{Q}(\sqrt{d}))$ and $\mathrm{Reg}(E^{(d)}/\mathbb{Q})$

H. (arXiv: 2507.20297)

For E non-CM, and d satisfies the Heegner condition.

- Handling some log contribution to get one-sided central limit theory for $\log \mathrm{Reg}(E/\mathbb{Q}(\sqrt{d}))$ and $\log \mathrm{Reg}(E^{(d)}/\mathbb{Q})$.
- Using Hölder's inequality to show lots of d such that $\mathrm{Reg}(E/\mathbb{Q}(\sqrt{d}))$ and $\mathrm{Reg}(E^{(d)}/\mathbb{Q})$ have size $\gg \sqrt{|d|}$.

$$\Omega_{E/\mathbb{Q}(\sqrt{d})} = \Omega_E^+ \cdot \Omega_{E^{(d)}}^+.$$

Order of imaginary period (Pal 2012)

For negative square-free $(d, 2N) = 1$,

$$\Omega_{E^{(d)}}^+ = \frac{\tilde{u}(d)}{\sqrt{|d|}} c_\infty(E^{(d)}) \Omega_E^-$$

with some $\tilde{u} \in \frac{1}{2}\mathbb{Z}$ decided by E, and $c_\infty(E^{(d)})$ denotes the number of connected components of $E^{(d)}(\mathbb{R})$, which is either 1 or 2.

Uniform boundedness theorem

H. (arXiv: 2507.20297)

For d satisfies the Heegner condition, assuming the BSD conjecture, there exist two constants C_1, C_2 depending on E such that

$$C_1 \leq \#Ш(E/\mathbb{Q}(\sqrt{d})) \prod_{v \text{ finite}} c_v(E/\mathbb{Q}(\sqrt{d})) \leq C_2.$$

Moreover, when $L(\frac{1}{2}, E) \neq 0$, this result also applies to $\#Ш(E^{(d)}/\mathbb{Q}) \prod_{p \text{ prime}} c_p(E^{(d)}/\mathbb{Q})$.

Thank you !